DATA PROTECTION POLICY

Policy Statement: The Policy is framed to protect Data at IEC University seeks to maintain and preserve the academic and work environment data. The Policy will also apply to outsiders and residents, of the University to the extent specified in these rules and procedures.

DEFINITIONS

I. "Students" includes regular students as well as current day scholars of the University.

II. 'Teaching staff' includes any person in the staff of the University, who is appointed to a teaching and/or research post, whether full time, temporary, ad-hoc, part-time, visiting, honorary, or on special duty or deputation and includes employees on casual basis.

III. 'Non-Teaching Staff' includes any person on the staff of IEC University, who is not included in the teaching staff. This category includes employees who are full-time, temporary, ad-hoc, part-time, visiting honorary, or on special duty or deputation, and the ones employed on a casual or project basis.

IV. "Member of the University" includes all those listed in categories I – III above.

V. "Resident" includes any person who is a temporary or permanent resident of any of the accommodations or premises allotted to him / her as an employee of the University.

VI. "Outsider" includes any person who is not a member of the University or a resident. It also includes, but is not limited to, any private person offering residential and other facilities to students, teaching staff or non-teaching staff of the University.

VII. "Campus" includes all places of work and residence in the IEC University. It includes all places of instruction, research and administration, as well as hostel, health centers, sports grounds, staff quarters and public places.

VII. Words used in Data Protection
(i). "access" with its grammatical variations and cognate expressions means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network;
(ii) "addressee" means a person who is intended by the originator to receive the electronic record but does not include any intermediary;

(iii). “electronic signature” with its grammatical variations and cognate expressions means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of electronic signature];
(iv) “asymmetric crypto system” means a system of a secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature;
(v) “communication device” means cell phones, personal digital assistance or combination of both or any other device used to communicate, send or transmit any text, video, audio or image;
(vi) “computer” means any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network;
(vii) “computer network” means the inter-connection of one or more computers or computer systems or communication device through—
(a) the use of satellite, microwave, terrestrial line, wire, wireless or other communication media; and
(b) terminals or a complex consisting of two or more inter-connected computers or communication device whether or not the interconnection is continuously maintained;
(viii) “computer resource” means computer, computer system, computer network, data, computer data-base or software;
(ix) “computer system” means a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files, which contain computer programmes, electronic instructions, input data, and output data, that performs logic, arithmetic, data storage and retrieval, communication control and other functions;
(x) “cyber cafe” means any facility from where access to the internet is offered by any person in the ordinary course of business to the members of the public;
(xi) “cyber security” means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorised access, use, disclosure, disruption, modification or destruction;
(xii) “data” means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts, magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer;
(xiii) “digital signature” means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3 of Information technology Act 2000;

(xiv) “electronic form” with reference to information means any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device;
(xv) “electronic record” means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche;
(xvi) “electronic signature” means authentication of any electronic record by a subscriber by means of the electronic technique specified in the Second Schedule and includes digital signature;
(xvii) “function”, in relation to a computer, includes logic, control, arithmetical process, deletion, storage and retrieval and communication or telecommunication from or within a computer;
(xviii) “information” includes data, message, text, images, sound, voice, codes, computer programmes, software and data-bases or micro film or computer generated micro fiche ;

SCOPE OF THE POLICY

DATA PROTECTION

MEANING

Use of techniques such as file locking and record locking, database shadowing, disk mirroring, to ensure the availability and integrity of Data is called DATA PROTECTION

HOW TO PROTECT OUR DATA

Applications can always be reinstalled, but your data is the most important thing on your computer or network. Here's a look at 10 ways you can protect that data.

1. **Save as you work.** You should always save your work as you go and learn how to use the 'auto-save' features in your application.
2. **Make a backup**. Before you make changes to critical data always make a duplicate. Even if you just made a backup yesterday - make another.
3. **Keep a copy of your data offsite.** Diligently backing up your data is good practice but keep a copy of your data offsite. If there were a fire or other disaster your onsite data backup could be lost as well.
4. **Refresh your archives.** Years ago you archived your data to a zip drive. Now you decide to use that data as a baseline - are you sure there is still a zip drive that can read your data? As technology changes, it is a good idea to transfer your data to a current data storage standard so that you aren't stuck with irretrievable data.
5. **Never open email attachments by habit.** If your email reader has an option to automatically open attachments you should disable that feature.

Always run any attachments and downloaded files through a virus scanner first.

6. **Never trust disks from other people**. Anytime you receive a file on any type of media check it first for viruses!
7. **Update!** Make sure you have the latest updates for your software - especially for your virus checking software. Make it a habit to regularly check for updates and enable automatic updates for software that offers that feature.
8. **Protect your passwords.** Your USERID is your identity. The key to your identity is your password. Anytime your account accesses the network you are responsible for any activity from that account!
9. Remember: change your password on a regular basis.
10. **Protect your computer.** Use a secure operating system which requires users to be 'authenticated'. As an added benefit these operating systems also restrict what individual users can see and do on the system.
11. **Perform regular maintenance.** Learn how to use the utilities that diagnose your system for problems. It is a good idea to run a disk-scanning program, defragment your harddrive, or whatever else your system might need. These utilities can prevent little problems from becoming big problems, and will keep your system running at top speed.

Trouble shots

In case of any trouble, IT Manager should be consulted after sending the problem to senior officer of IEC University

LAW ON DATA PROTECTION IN INDIA

Information Technology Act 2000

Indian Penal Code 1860

INDIAN EVIDENCE ACT 1872